EXAMENSARBETE

Våren 2015

Sektionen för hälsa och samhälle
Kriminologi

Medias rapportering av IT-relaterade brott

Författare

Fredrik Lundgren

Aurora Pirraku Eriksson

Handledare

Joakim Thelander

Examinator

Jonas Ringström

Högskolan Kristianstad | www.hkr.se

Abstract

I uppsatsen har problemställningen varit om det finns det någon skillnad mellan hur olika typer av publikationer, Aftonbladet.se och IDG.se, väljer att publicera nyheter om IT-relaterade brott. Metoden har varit att genom en kvantitativ innehållsanalys använda en kodningsmanual för att undersöka relevanta artiklar från två mediehus, Aftonbladet.se, som har en webbtidning och IDG.se, som har en rad teknikinriktade (speciellt datorteknik) tidningar på webben. Vi har valt att hämta artiklar från åren 2012 till och med 2014.

Den teori som valts som grund för analysen i uppsatsen är den så kallade skandalteorin där en skandal karaktäriseras av att något exceptionellt inträffar genom att en eller flera personer inte uppför sig som han eller hon borde, vilket resulterar i ett förtroendebrott.

Under perioden 2012-2014 har utvecklingen av artiklar som handlar om IT-relaterade brott legat mellan 150 – 250 artiklar per år med något fler från IDG.se. Aftonbladet.se har en publik som utgörs av privatpersoner där den ”säljande” skandalen också mer naturligt är en händelse där en privatperson är offret medan IDG.se har en publik som i högre grad utgörs av företag och offentliga organisationer eller de som är intresserade av teknik i relation till företag.

Nyckelord

IT-relaterade brott, cyberbrott, IT-brott, IDG.se, Aftonbladet.se, artiklar

Innehållsförteckning

Inledning

IT-relaterade brott har funnits så länge datorer använts i någon ekonomiskt och socialt relevant omfattning. Det är alltså inte något nytt begrepp och Brottsförebyggande rådet rapporterade om brottskategorin redan under tidigt 1980-tal (Brå 2002, s. 5). Rapportering om denna brottslighet varierar över tid och mellan olika media. I dagens samhälle där allt färre läser dagstidningar utan istället väljer från ett stort smörgåsbord av media med olika inriktningar, finns möjligheten att i mycket stor omfattning välja att inte bara läsa det man är intresserad av, utan också välja informationskanaler som endast presenterar den nyhetsinriktning läsaren finner intressant och utelämna allt annat. Detta beteende ger upphov till ett fenomen som kallas mediabubbla. En mediabubbla kan få mer eller mindre allvarliga konsekvenser – alltifrån att läsaren endast möts av extremistiska politiska budskap från likatänkande, till att läsaren missar någon mindre viktig aspekt av samhällsrapporteringen. Oavsett om konsekvensen av mediabubblan blir allvarlig eller oviktigt trivial, så antar vi att mekanismen i hur mediabubblan uppstår är likartad. Finns det någon skillnad i frekvens och ämne i hur IDG.se, som har mer fackinriktade tidningar och Aftonbladet, som är en bredare tidning, rapporterar om IT-relaterade brott? Hur stor är den skillnaden i så fall och hur utvecklas rapporteringen med tiden? För den intresserade kan också uppsatsen ses som en mall eller inspiration för hur en till formen liknande sökning och analys kan göras, oavsett om sakfrågan berör IT-relaterade brott eller ej.

Syfte och frågeställningar

Syftet med uppsatsen är att studera medias rapportering av IT-relaterade brott över tid, och studera skillnader i rapportering mellan olika publikationer. Våra frågeställningar: mellan IDG.se och Aftonbladet.se, är det skillnad i frekvens i rapportering av olika kategorier av brott? För att samla data från svensk press använde vi IDG.se, som publicerar fack- och teknikinriktade tidningar och Aftonbladet.se, som är en vardaglig nyhets- och nöjestidning. Dessa valdes som datakällor främst eftersom de är stora och representativa i Sverige och eftersom de båda hade sökfunktioner för artiklar där man kan söka flera år bakåt i tiden baserat på nyckelord. Vår frågeställning är följande:

> ”Om det finns någon skillnad mellan hur olika typer av publikationer, Aftonbladet.se och IDG.se, väljer att publicera nyheter om IT-relaterade brott?”

En förhoppning är, att arbetet kan påvisa ett mycket enkelt exempel av hur den på senare tid omtalade "mediabubblan" kan ge individer olika fönster mot verkligheten - hur skiljer sig rapporteringen av cyberbrott (eller annat ämne) för dem som väljer en nyhetskälla utifrån en viss ämnesinriktning jämfört med mer breda, traditionella nyhetskällor? När de flesta läste dagstidningen, exponerades den publiken för samma saker. Även om en enskild mediekonsument alltid valde att inte läsa exempelvis kultursidorna, uppstod ändå en medvetenhet om att detta ämne existerade och att en tillräcklig mängd människor måste vara intresserade av detta ämne, annars skulle det inte fått spaltutrymme i tidningen. I dag finns oändliga möjligheter att inte bara välja inriktning på sin nyhetsrapportering utan också möjlighet att välja bort all sorts nyhetsrapportering som inte upplevs som intressant. I vår uppsats demonstreras hur.

Bakgrund och tidigare forskning

Vad är cyberbrott/cybercrime? I Future Challenges of Cybercrime, Vol. 5, tas olika sätt upp att definiera cyberbrott. Där placeras olika definitioner på en skala, där mer specifika definitioner är på ena sidan och mer generella definitioner på den andra. I den ena änden av skalan räknas som cyberbrott endast medvetna attacker med avsikt att skada sårbara datorsystem och utnyttjande av fel i dem. På den andra, mer generella sidan, räknas allt som cyberbrott där på något sätt datorer eller Internet används. (Finnie, Petee, Jarvis 2010.)

I boken Cybercrime and Society sammanfattar Majid Yar (Yar 2013) begreppen.
Redan i inledningen konstaterar Majid Yar att den här andra utgåvan av boken har behövt en rejäl uppdatering sedan den första utgåvan 2005. Då var Facebook i sin linda och nu har den sociala plattformen fullständigt exploderat, vilket gör att området rör på sig i en ovanligt snabb takt (Yar 2013, förord till andra utgåvan).

Internets kriminella dimensioner har i mångt och mycket skapats och förstärkts av massmedia. Yar tar upp en annan forskare, Dowland, som undersökte två, väl ansedda, tidningar i Storbritannien och visade att datorrelaterad brottslighet förekom i snitt med två reportage i veckan under den granskade perioden på två och ett halvt år. Förutom traditionell pappersmedia och teve-sänd media står idag Internet för merparten av rapporterade inslag om cyberbrott. Medias bidrag till beskrivningen av utvecklingen inom området cyberbrott blir ett viktigt bidrag för fortsatt kriminologisk forskning om vad cyberbrottslighet består i och hur begreppet ska definieras. En fara i sammanhanget kan vara att medias presentationer vanställer verkligheten

bakom den brottslighet som sker på Internet i stället för att bidra till en balanserad förståelse av området (Yar 2013, s.4).

Cyberbrottslighet handlar inte om någon specifik kriminell aktivitet utan i stället om en rad kriminella aktiviteter som har det gemensamt att de genomförs i en unik elektronisk miljö, det så kallade cyberspace. Yar har för avsikt att förklara varför cyberbrott är kvalitativt annorlunda än annan kriminalitet (Yar 2013, s. 5-6).

Ett stort problem då cyberbrottsligheten ska studeras är att det inte finns någon enhetlig definition av vad cyberbrott är. Även om begreppet cyberbrott används frekvent i den politiska debatten, av media och i den akademiska världen finns inte cyberbrott som ett särskilt begrepp i straffrätten. (Brå 2002, s. 11) Brottsförebyggande rådet, en statlig myndighet, skriver i sin rapport från 2002 att antagligen kommer termen IT-relaterad brottslighet i framtiden sakna betydelse, i takt med att IT genomsyrar allt i samhället. (Brå 2002, s. 45) I stället för att förklara cyberbrott som ett särskilt definierat fenomen kan begreppet i stället handla om olagliga och i övrigt avvikande aktiviteter som utförs i ett globalt elektronisk nätverk. En avgränsning i den här uppsatsen blir, precis densamma som i Yars bok, de aktiviteter som är kriminaliserade enligt straffrätten. Det görs ibland skillnad på aktiviteter som är beroende av Internet för att leda till brott och andra aktiviteter som skulle kunna leda till brott oavsett om Internet förekom eller inte. En del polisiära organisationer, som exempelvis Storbritanniens Hi-Tech Crime Unit, använder den här skillnaden för att beskriva å ena sidan traditionella brott med hjälp av ”nya” verktyg och ”nya” brott med ”nya” verktyg. Nackdelen med den här uppdelningen av brottsligheten är att den bara utgår från själva tekniken och inte från förhållandet mellan gärningsmännen och offren. Därför kan det vara ett alternativ att dela in cyberbrott i redan etablerade brottskategorier (Yar 2013, s. 9-10).

I betänkande, Informations- och cybersäkerhet i Sverige (Arrland et al, 2015) nämns förutom “cybersäkerhet” också “informationssäkerhet”. Skillnaden mellan informationssäkerhet och cybersäkerhet definieras som att informationssäkerhet handlar om dels tekniskt skydd för information, standardisering och policy. Cybersäkerhet definieras som mer strategiskt och nationellt med internationell räckvidd - normer och folkrätt är relevanta ord tillsammans med cybersäkerhet, däremot inte med informationssäkerhet. (I betänkandet nämns också att informationssäkerhet, eller “information security” *ändå* används i internationella sammanhang som ett diplomatiskt kodord av stater med en repressiv hållning till hur Internet ska styras och kontrolleras.) (Arrland et al 2015, s. 40).

I betänkandet konstateras också att det inte finns någon formell konsensusdefinition av ord med förledet "cyber", inte ens på engelska, men att vissa ord ändå används på svenska i säkerhetspolitiska och utrikespolitiska sammanhang, exempelvis cybersäkerhet, cyberrymden, cyberpolitik etc. International Telecommunications Union definierar cybersäkerhet ganska generellt, som något som går ut på att en organisations säkerhetsegenskaper ställs mot relevanta risker i cybermiljön. Generella säkerhetsegenskaper är tillgänglighet, integritet och konfidentialitet. Författaren konstaterar att så länge det gäller inhemsk myndighetsutövning går det säkert bra att utbytbart använda cybersäkerhet och informationssäkerhet, men att så fort det gäller ett större internationellt perspektiv bör istället cyber-förledet användas. (Arrland et al 2015, s. 42-43).

Pollack beskriver framväxten av ett Law- and Order-samhälle via ett samspel mellan media och polis. Beskrivningar i media föder krav på hårdare tag från polisens och rättsväsendets sida, och deras insatser hittar då fler gärningsmän och brott av den föreskrivna typen. (Pollack, 2001 s. 33) Pollack talar här om traditionella brott. Förr i tiden var de flesta traditionella brott lokala, utförda i den jurisdiktion där polisen och myndigheterna befinner sig. Men cyberbrottet är ofta distribuerat över en geografiskt, politiskt och juridiskt stor yta dit polis och nationella myndigheter inte har räckvidd. Därför kanske cirkeln mellan polis och media delvis är bruten, i alla fall vad gäller icke lokala cyberbrott? Media kan beskriva problemet, men polisen kan inte som förr svara lika kraftfullt som den kunde på mer lokala fenomen.
Pollack tar upp temat med skillnaden mellan kvalitets- och fackpress gentemot övrig media. Där nämns att skillnaden i volym av brottsrapportering kan vara stor mellan olika typer av publikationer. (Pollack 2001, s. 71)

Medierapporteringen kan också påverka uppfattningen om vad som är brottsligt, och påverka lagstiftarna i någon riktning. En grupp med till synes litet inflytande i samhället kan under rätt omständigheter få en stor påverkan. (Pollack 2001, s. 42)
Den brottslighet som uppmärksammas i media, tenderar också att bli den brottslighet som rapporteras till Polisen i högre utsträckning, utan att för den skull brottsligheten själv skulle öka. (Pollack 2001, s. 36) Det är något som också har inspirerat oss till de frågeställningar vi tar upp i uppsatsen.

David S. Wall (Wall, 2008) definierar cyberbrottslighet i tre kategorier, ordnade i en skala. Den första nivån på skalan är brott som använder "internet" eller "nätverket" för kommunikation,

men som utan tillgång till internet ändå skulle fortsätta, men med något annat medium för kommunikation. Den första nivån är traditionella eller vanliga brott. I nästa nivå hamnar brott som skulle gått att genomföra utan internet, men som tack vare internet går att utföra i en mycket större skala. Dessa kallas för hybrid-brott. Den tredje och sista kategorin, kallas för sanna cyberbrott ("true cybercrime") och utgörs av brott som inte varit möjliga utan nätverkseffekten. (Wall 2008, s. 55)

Jewkes gör en liknande distinktion, mellan datorstödda brott ("computer assisted") och datororienterade ("computer oriented") brott. Den första termen refererar till brott som tack vare Internet är lättare att utföra, den andra termen, "computer oriented" refererar till brott som är möjliga tack vare Internet-teknik. (Jewkes Y 2011, s. 242)

En annan dimension av cyberbrott är cyberterrorism och cyberkrig. Media i västvärlden anklagar Kina för att vara en stor källa till cyberbrott, cyberterrorism och cyberkrig. En del av anklagelserna har antagligen sin grund i en västlig rädsla för Kinas expansion på marknader tidigare kontrollerade av västvärlden. (Jewkes Y 2011, s. 243 - 244)

Det gäller att vara kritisk till hur olika media presenterar cyberbrott, och brott i allmänhet. Till exempel har traditionell massmedia en tendens att undvika att gräva i nätverk av relationer, eftersom det kan skada karriären för den enskilda journalisten. (Levi M. 2008, s. 376)

I massmedia har rapporteringen ofta en hysterisk och uppförstorande prägel. (Levi M. 2008, s. 374) Det passar in med observationen hos D.S. Wall, att det finns en mytbildning kring cyberbrott som bättre passar in med fiktionen och eventuellt med hackerkulturen i det tidiga 1990-talet och innan, än med dagens verklighet. Dagens cyberbrottslingar har mycket lite gemensamt med det ensamma hacker-geniet eller med hårt kontrollerade grupper av organiserad brottslighet. (D. S. Wall 2008, s. 48)

Jewkes poängterar också att fast de cyberbrott massmedia helst rapporterar om liknar en actionfilm från Hollywood, så är det så att de cyberbrott som mest troligen påverkar oss är vardagliga, enkla cyberbrott. Jewkes tar upp olaglig spridning av upphovsrättsskyddat material och rekrytering av medlemmar till radikala grupper tack vare det effektiva sättet att hitta likasinnade på Internet. Även exempelvis kreditkortsbrott, identitetskapning och bedrägerier tas upp. Tack vare det ökade avståndet mellan offer och förövare går den skyldiga lättare fri. Ett

annat trivialt men allvarligt exempel är när brittiska skatteverket slarvade bort två CD-skivor med uppgifter om 25 miljoner människor. (Jewkes Y. 2011, s. 242, 247, 248, 253.)

Det är viktigt att kontinuerligt utvärdera våra egna ståndpunkter - det som förut togs för allmän sanning kan ha förändrats inom bara några år. (Wall 2008, s. 51.) Samtidigt bygger alla parter gradvis mer kunskap, tack vare forskningen. (Wall 2008, s. 55)

Teori

När det gäller cyberbrottslighet eller IT-relaterad brottslighet kan det här med bakomliggande teorier skilja sig beroende på vilken traditionell brottstyp det handlar om. Det kommer naturligtvis finnas vissa teorier som bättre kan kopplas till brott som begås med tanke på ekonomisk vinning som bedrägeri och i vissa fall dataintrång. Andra teorier kan i stället bättre förklara IT-relaterade barnpornografibrott och grooming. Den fortsatta teoriredogörelsen kommer inte beröra alla bakomliggande teorier för de olika traditionella brottstyperna utan i stället fokusera på en teori som kan förklara varför media väljer att rapporter och publicera vissa brottstyper men inte andra.

Såväl tidningen Aftonbladet.se som den mer fackinriktade nätsajten IDG.se med sina tidningar behöver en publik för att publiceringen av nyheter och artiklar ska vara lönsam. När det gäller rapportering av brott och brottslighet ligger det nära till hands att tala om skandaler. En skandal karaktäriseras av att något exceptionellt inträffar genom att en eller flera personer inte uppför sig som han eller hon borde, vilket resulterar i ett förtroendebrott (Wästerfors 2008, s. 74-75).

Själva handlingen där någon eller några inte uppför sig på ett, för publiken (eller i vårt fall läsarna), acceptabelt sätt blir såväl en förutsättning för skandalen. Skandaler handlar inte allt för sällan om brott och rättsprocesser även om det inte är säkert att den klandervärda handlingen uppmärksammas oaktat ett brott eller inte. Om publiken väljer att avvisa den exceptionella händelsen och förtroendebrottet riskerar skandalen att sjunka ihop så därför behövs det ytterligare kännetecken för att definiera en skandal. En skandal behöver en publik som bevarar skandaletiketten (Wästerfors 2008, s. 75-76).

Idag kan publikens interaktion med olika typer av media vara mer eller mindre subtil och ibland förser media oss med olika samtalsämnen och metaforer på ett nästintill osynligt sätt. Då läsarens intresse egentligen har fokus på något helt annat kan en kort nyhetsnotis eller artikel i

förbifarten uppmärksamma läsaren på en skandal som sedan kan leda till korta hänvisningar i samtal, debatter och argumentation (Åkerström 2008, s. 81).

Skandalteorin passar bra för att kunna analysera hur två olika medietyper, Aftonbladet.se respektive IDG.se, väljer att rapportera IT-relaterade brott. Basen blir själva brottet som är den händelse som för respektive media är tillräckligt exceptionell för att utgöra en skandal för den aktuella publiken. Genom analysera vilka brott som publiceras av Aftobladet.se och IDG.se samt vilka offer som presenteras i de olika artiklarna kan sedan skandalteorin användas för att förklara resultatet.

Styrkan med skandalteorin är att den kan användas när en publik förväntas ha en reaktion på en viss exceptionell händelse och att det vidare kan finnas ett intresse för media att publicera nyheter och artiklar om vissa IT-relaterade brott. Något som vi kan använda för att besvara frågeställningen om det finns någon egentlig skillnad mellan hur olika typer av publikationer, Aftonbladet.se och IDG.se, väljer att publicera nyheter om IT-relaterade brott med avseende på brottstyper och offer.

Svagheterna med skandalteorin är att det egentligen inte går att avgöra om det finns andra skäl till varför media väljer att publicera nyheter om IT-relaterade brott. Det är med andra ord inte säkert att en skandal innebär tillräckligt många läsare för att innebära ett incitament för redaktionen att publicera artikeln för att öka intäkterna.

Metod

För att på bästa sätt få ett svar på vår frågeställning om det finns någon skillnad mellan hur olika typer av publikationer väljer att publicera nyheter om IT-relaterade brott, med avseende på brottstyper och brottsoffer, väljer vi att göra en kvantitativ innehållsanalys. Den här metoden är vanlig i samband med medieforskning och kan svara på frågor om *vem* som beskrivs, *vad* som rapporteras, *var* undersökningen har gjorts m.m. När det gäller vår undersökning är det i första hand *vad* som rapporteras som är intressant när det gäller brottstyper och offer (Bryman 2008, s. 285).

En kvantitativ innehållsanalys är en forskningsteknik som rör en objektiv, systematisk och kvantitativ beskrivning av det konkreta eller manifesta innehållet i kommunikationen. Det viktiga är följaktligen egenskaperna objektivitet och systematik. Objektiviteteten innebär att i förväg specificera hur olika delar av råmaterialet ska hänföras till olika kategorier, vilket kan

liknas vid ett så kallat observationsschema. Systematiken innebär vidare att reglerna för innehållsanalysen används på ett konsekvent sätt för att säkerställa att varje form av skevhet och felkälla blir så liten som möjligt (Bryman 2008, s. 282).

När det gäller innehållsanalys av massmedia är ett syfte att undersöka trender för att se hur intresset för ett visst tema har utvecklats i rapporteringen. Urvalet blir också viktigt för att begränsa innehållsanalysen och det gäller särskilt i samband med massmedialt innehåll. Det vanligaste är att välja en eller två media för att senare göra ett urval inom ramen. Valet av tidsperiod kan bero på flera olika faktorer där det i vissa fall kan vara aktuellt att starta när en särskild händelse inträffar medan det i andra fall kan vara mer relevant att titta på ett fenomen ur ett mer generellt perspektiv där valet av tidsperiod också blir en mer öppen fråga (Bryman 2008, s. 284-286).

Inom ramen för vår innehållsanalys har vi valt att fokusera på rikstäckande webbmedia i form av Aftonbladet.se samt en samlingssida http://www.idg.se från mediahuset IDG som rapporterar från sina branschspecifika media (Som rapporterar nyheter från CIO Sweden, Cloud Magazine, ComputerSweden, Internetworld, IT i Vården, IT24, M3, Macworld, Pc för Alla, Säkerhet24, Techworld och IT.Branschen). Vårt urval blir således alla artiklar som matchar aktuellt kodschema från de senaste 3 åren för att kunna se om det finns en särskild trend inom området IT-relaterad brottslighet.

Vad som ska räknas i samband med innehållsanalys beror vanligen på den frågeställning som ligger till grund för forskningen. Personer och egenskaper hos personer är ofta viktiga att koda i samband med massmedial nyhetsrapportering. Det här innebär ofta att vem som har skrivit texten blir viktigt att få med liksom vilket sammanhang texten förekommer i (intervju, presskonferens, rättsfall, m.m.). När det gäller hur mer samhällsvetenskapliga fenomen, som kriminologi behandlar, beskrivs i media kan det vara viktigt att dessutom notera upplysningar om den forskare som uttalat sig i artikeln och om texten hör samman med någon vetenskaplig konferens eller en pressrelease i samband med presentation av nya forskningsresultat (Bryman 2008, s. 287-288).

Det är vanligt att dela in innehållsanalysen i olika teman och ämnesområden där syftet är att kategorisera de företeelser som är av största intresse för analysen. Även om kategorisering förefaller okomplicerad är det viktigt att utgå från ett tolkande perspektiv då kodningen är av ett tematiskt slag. En ytterligare tolkningsnivå som kan användas är att analysera dispositionen

i de texter som ingår i innehållsanalysen. Ett syfte kan vara att få en bild av om journalisten är välvilligt eller negativt inställd till det som beskrivs i texten. Det är också vanligt att dispositionen kommer i fokus då innehållsanalysen handlar om att koda ideologier, åsikter och principer. I den här uppsatsen kommer vi dela in IT-relaterade brott i olika teman för att lättare kunna se utvecklingen inom området. De teman vi väljer kommer huvudsakligen bygga på den indelning som svenska polisen gör och även den indelning som Majid Yar gör i boken Cybercrime and Society där en första lista kan se ut enligt följande:

1. Dataintrång
2. Datorbedrägeri
3. Barnpornografibrott
4. Näthat
5. Bedrägerier
6. Gromning
7. Phishing
8. Skimning
9. Hacking och intrång
10. Trojaner

Genom att bygga upp kodningsschemat med dimensionen ”Samlingsbegrepp” kan vi se om det finns något särskilt begrepp som eventuellt används för att gruppera de aktuella brottstyperna. I övrigt har brottstyperna valts för att så långt som möjligt täcka in artiklar som handlar om IT-relaterade brott. För inte bara välja en myndighets, polisens, uppfattning om vad som ska räknas som ett IT-relaterat brott har vi också valt att ha med forskaren Majid Yars lista av brott inom området.

Kopplingen till skandalteorin bygger på att en skandal är en tillräckligt exceptionell händelse för att Aftonbladet.se eller IDG.se ska välja att publicera en nyhet. Därmed blir händelsen värd att räknas i innehållsanalysen då den kan svara på vår frågeställning med avseende på vad som har rapporterats relaterat till brottet (Bryman 2008, s. 287).

Däremot kommer vi inte att fokusera på dispositionen i de artiklar vi har för avsikt att inkludera i vår innehållsanalys.

Vi använder ett kodningsschema och en kodningsmanual. En sammanhållande lista med det aktuella kodningsschemat kommer att fyllas i för varje artikel om IT-relaterade brott som ska kodas. Vidare kommer kodningsmanualen att innehålla alla olika kategorier för respektive dimension som ska kodas. Själva kodningsmanualen är viktig då den ger kodaren en fullständig lista över alla kategorier som hör till de olika dimensionerna i kodningsschemat och blir därmed grunden för de vägval som gäller vid ifyllande av blanketten (Bryman 2008, s. 291-292).

I denna uppsats gäller följande kodningsschema och kodningsmanual:

#	**Dimension**	**Kategorier**
1.	Media	(1) Aftonbladet (2) http://www.idg.se
2.	År	(1) 2012 (2) 2013 (3) 2014
3.	Samlingsbegrepp	(1) Cyberbrott (2) IT-brott (datorintrång eller datorbedrägeri) (3) IT-relaterad brottslighet (alla övriga brott) (4) Kan inte avgöras
4.	Brottets art enligt Polisen	(1) Dataintrång (2) Datorbedrägeri (3) Barnpornografibrott (4) Näthat (5) Bedrägeri (6) Gromning (7) Phishing (8) Skimning (9) Hacking och intrång (10) Trojaner
5.	Brottets art enligt Majid Yar	(1) Hacking och cracking (2) Politisk hacking och cyberterrorism (3) Pirater och brott mot immaterialrätt (4) Bedrägerier (5) Brottsliga texter och pornografi (6) Förtal och hets mot folkgrupp

6.	Myndighet som i första hand nämns i artikeln	(1) Polisen (2) Åklagarmyndigheten (3) Domstolsverket (4) Brå (5) Tullverket (6) Regeringen (7) Annan (8) Ingen

Avslutningsvis en sammanfattning av innehållsanalysens starka och svaga sidor. När fördelarna med en innehållsanalys utvärderas väger det tungt att metoden ofta beskrivs som en objektiv analysmetod. Innehållsanalysen gör det också lätt att genomföra longitudinella analyser och det är en flexibel metod som kan användas på många olika typer av ostrukturerad information (Bryman 2008, s. 296).

Det finns naturligtvis också en del negativa aspekter med innehållsanalysen som metod. Bland annat blir metoden aldrig bättre än de källdokument metoden bygger på. I den här uppsatsen handlar det om artiklar från media som, om inte den aktuella webbsidan just blivit föremål för en cyberattack eller annat IT-relaterat brott, bör uppfylla kraven på autenticitet, trovärdighet och representativitet. Ett annat problem med innehållsanalyser är att det är svårt att utforma en kodningsmanual som inte bygger på en viss tolkning från kodarna. Innehållsanalyser blir ibland anklagade för att vara ateoretiska då det som mäts är det som går att mäta och inte det som är av teoretisk vikt. Det här är något som det gäller att vara vaksam på även i den här uppsatsen (Bryman 2008, s. 296-297).

En relaterad invändning hittar vi hos (Pollack 2001, s. 69), mot kvantitativa undersökningar - varje text eller artikel finns i ett unikt sammanhang, vilken publik har den, hur stor, hur tolkar publiken texten, vilken placering och exponering har texten i publikationen?

Datainsamling

Datainsamling av artiklar från nyhetssajten IDG.se och Aftonbladet.se gjordes med hjälp av ett program som automatiskt laddar ner artiklar från dessa publikationer och sammanställer dem i listor i flera format, i Excel-format, SPSS-format och i PDF-format. Sökningen gjordes med ett tidsintervall inom vilket artikeln ska vara publicerad, samt en lista av nyckelord. Vi använde intervallet från och med första januari 2012 till och med sista december 2014.

Nyckelorden som användes var:

"bedrägeri nätet", "bedrägeri internet", "bedrägeri web", "bedrägeri identitet", "bedrägeri online", "hets mot folkgrupp", "itbrott", "IT-brott", "ITbrott", "cyberkrim", "cyberkriminalitet", "cyber-kriminalitet", "cybercrime", "cyber-crime", "cyber-crime", "cyberbrott", "cyber-brott", "IT-relaterade brott", "IT-relaterad brott", "datorintrång", "dator-intrång", "dataintrång", "data-intrång", "datorbedrägeri", "dator-bedrägeri", "databedrägeri", "data-bedrägeri", "barnpornografi", "barn-pornografi", "näthat", "nät-hat", "groomning", "gromning", "grooming", "phishing", "phishning", "skimmer", "skimming", "skimmning", "hacking", "hackning", "trojan", "cracking", "cracker", "hacker", "cyberterror", "cyber-terror", "pirater", "förtal"

Sökningen gjordes med hjälp av tidningarnas egna sökformulär och resultatet är därför beroende av hur tidningens webbsida själv svarar på ett sökord. För att göra sökningen mer robust har därför ett antal uttalade varianter av sökorden lagts till i listan av nyckelord, enligt ovan. IDG.se är en utgivare av flera tidningar, men har ett gemensamt sökformulär för alla sina svenska tidningar. I varje sökresultat är det angett vilken tidning artikeln kommer ifrån. Aftonbladet.se har en egen söksida. En styrka med denna metod jämfört med att använda en allmän sökmotor är att vi inte blir beroende av att sökmotorn, som t ex Google, ska lyckas hitta varje artikel med det nyckelord vi söker på. Vi undviker ett led i kedjan där fel kan introduceras.

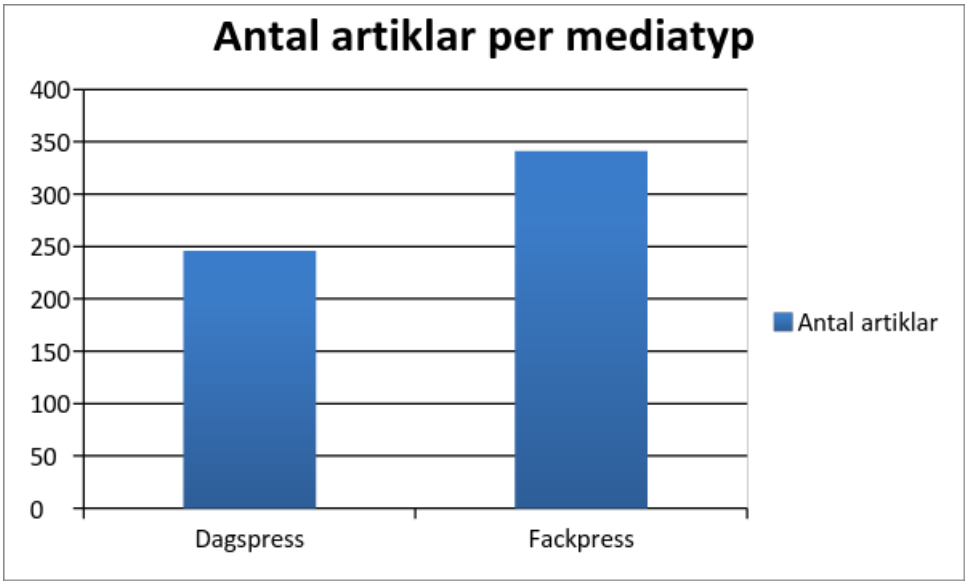
Programmet sammanställer artiklar publicerade inom tidsramen som angetts, men är i övrigt likvärdigt med att en mänsklig användare för hand skulle sammanställa samma lista av artiklar, men naturligtvis med mycket mindre risk för manuella fel. Det betyder inte att automatisk datainsamling inte har sina egna problem. Vi upptäckte ett fel i programmet som gjorde att inga sökresultat erhölls från IDG.se om nyckelord innehöll bokstaven å, ä, eller ö. Felet kunde rättas till och en ny körning göras, men det demonstrerar hur viktigt det är att vara ständigt kritisk till sina källdata.

Resultat

I den här uppsatsen har vi valt att undersöka utvecklingen av rapportering av IT-relaterad brottslighet i media. De media vi valt att fokusera på är dels Aftonbladet på nätet, http://www.aftonbladet.se, dels samlingssidan IDG på nätet, http://www.idg.se. IDG är en samlingssida för tidningarna CIO Sweden, ComputerSweden, PC för Alla, Internetworld, M3 och Techworld som alla är branschtidningar inom IT-området.

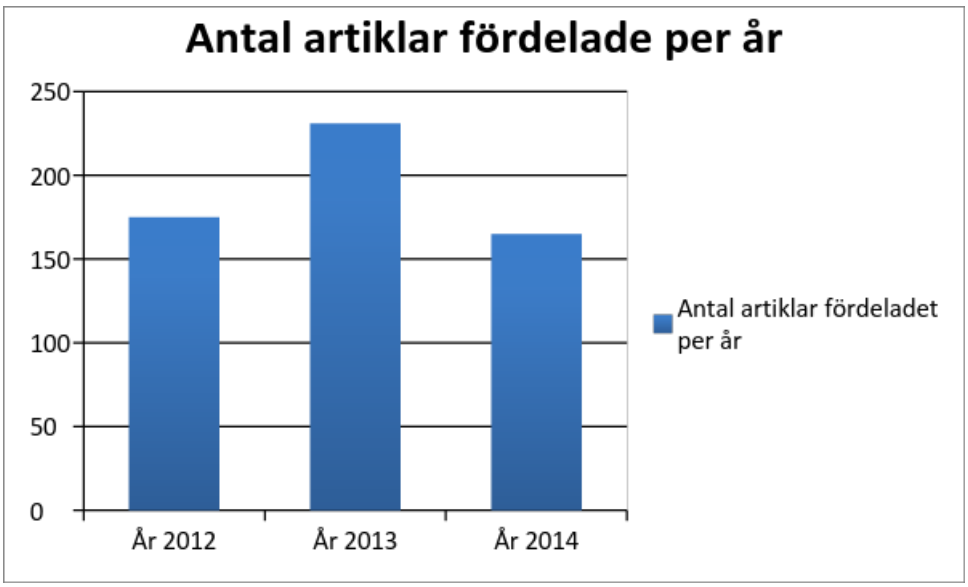
Genom att använda ett särskilt program för att automatiskt ladda ner artiklar från de utvalda publikationerna under den definierade perioden 2012-2014 har totalt 1980 artiklar kunnat sammanställas. Artiklarna har sedan jämförts mot och klassificerats enligt den kodningsmanual med tillhörande kodningsschema som redovisats i metodavsnittet. Resultatet blev att 571 artiklar återstod efter att 1409 artiklar rensats bort som irrelevanta för studien. Exempel på artiklar som rensats bort är dels artiklar som handlat om vanliga bedrägerier, sjöpirater utanför Somalias kust i stället för pirater inom IT-området och artiklar som ger allmänna råd om att förbättra säkerheten på Internet. En hel del artiklar har dessutom varit dubbletter och blivit bortrensade av det skälet.

Totalt har alltså 571 artiklar analyserats vidare enligt kommande redovisning. En första redovisning är totala antalet artiklar fördelade mellan Aftonbladet och IDG under 2012-2014.



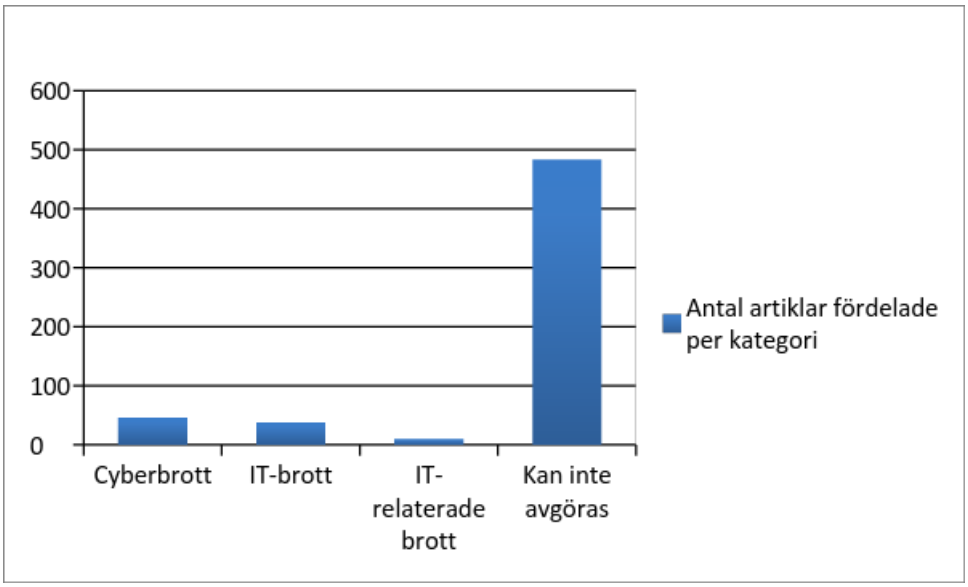
Antalet artiklar på Aftonbladet var 246 medan resultatet från IDG var 325 artiklar under perioden. Att IDG.se har fler artiklar under perioden är ett inte särskilt förvånande resultat, med tanke på att IDG just fokuserar på artiklar inom IT-området medan Aftonbladet har ett mycket bredare fokus.

Nästa sammanställning visar fördelning av artiklar per år under perioden 2012-2014.



Antalet artiklar var 175 år 2012, 213 år 2013 och 165 år 2014.

De begrepp som förekommer som kategorier i kodningsschemat är cyberbrott, IT-brott, IT-relaterade brott och en kategori för återstående "kan inte avgöras", där artikelinnehållet inte passar in för cyberbrott, IT-brott eller IT-relaterade brott. För de artiklar där det inte kan avgöras om brottet är kopplat till något av samlingsbegreppen har ändå artiklarna ett innehåll som rör brott med anknytning till IT, d.v.s. artiklarna handlar om någon/några av de olika brottstyperna (exempelvis hacking, gromning, m.fl.).



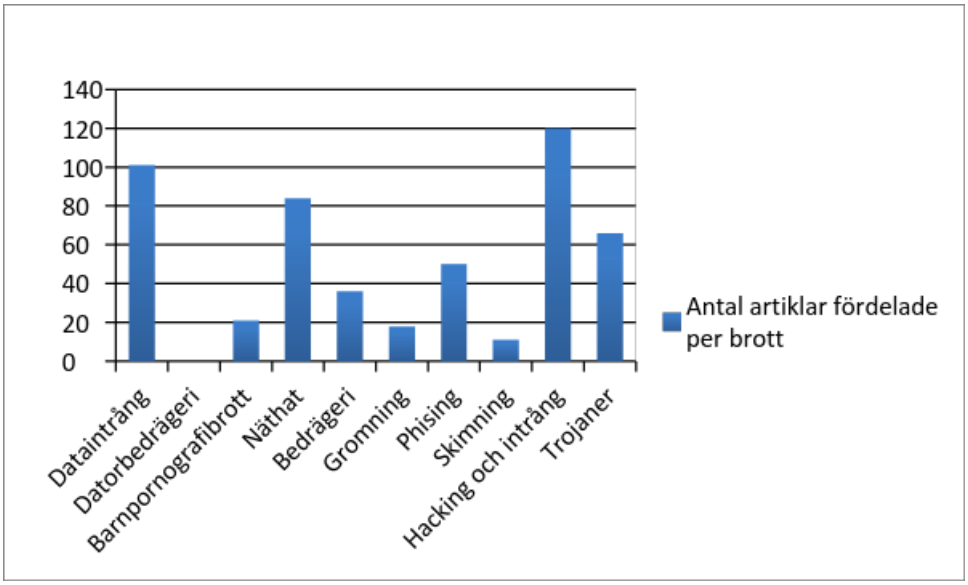
Av alla artiklar innehåller 483 stycken ett material som inte kan kopplas till något samlingsbegrepp. Endast 10 artiklar innehåller begreppet IT-relaterade brott och IT-brott förekommer i 38 artiklar medan cyberbrott förekommer i 46 artiklar.

Det är intressant att notera att en fjärdedel av artiklarna som innehåller samlingsbegrepp cyberbrott/cyberbrottslighet också handlar om EU. Följande är ett exempel på innehåll i den här typen av artiklar:

"EU-kommissionen höjde under gårdagen sin budget för cyberbrott med endast 14 procent. Under perioden 2007 till 2013 öronmärktes 350 miljoner euro för att bekämpa cyberbrott. Under perioden 2013 till 2020 ökades budgeten med endast 50 miljoner euro." (EU satsar inte tillräckligt på att bekämpa cyberbrott 2012).

Brottets art - detaljerat resultat

I det här avsnittet redovisas mer detaljerat resultat uppdelat bland annat beroende på brottets art och om det är en privatperson, offentlig verksamhet eller ett företag som blivit utsatt för brottet. En total sammanställning av hur artiklarnas innehåll är fördelade enligt polisens definition av brottets art redovisas först.



Flest artiklar enligt polisens definition av brottets art har dataintrång (101), näthat (84) och hacking och intrång (120). Nästa grupp är bedrägeri (36), phishing (50) och trojaner (66). Sista gruppen, med minst antal artiklar, är gromning (18), barnpornografibrott (21), skimning (11) och datorbedrägeri (0).

Att det inte förekommer en enda artikel som handlar om brottet datorbedrägeri kan bero på att många artiklar inte tar upp den formella brottsrubriceringen. Enligt brottsbalken 9 kap. 1 § andra stycket är databedrägeri också bara en variant av ett klassiskt bedrägeribrott och den gemensamma brottsrubriceringen är bedrägeri. Därmed kan flera av artiklarna som bland annat

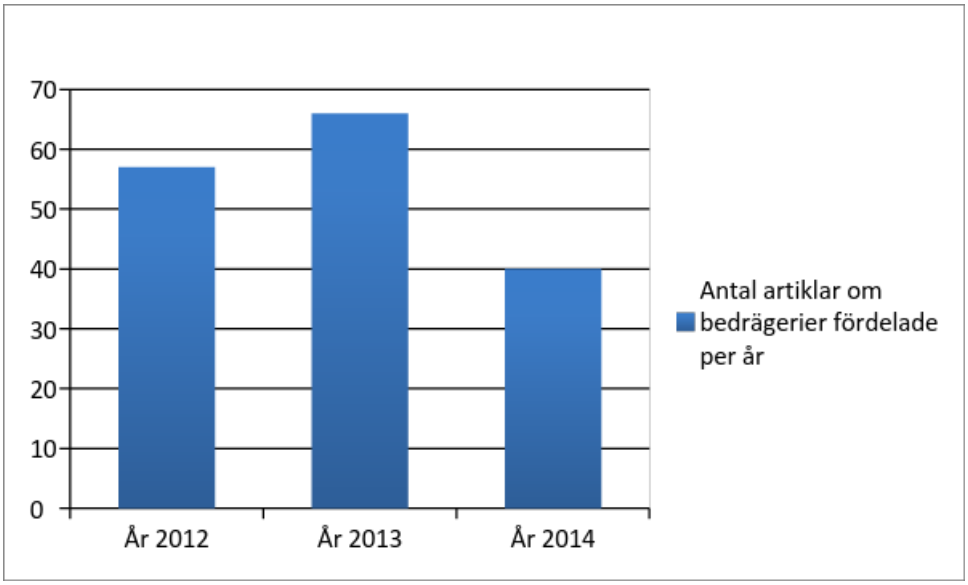
handlar om bedrägeri, phishing och trojaner i slutändan resultera i det polisen kallar för ett datorbedrägeri. Följande citat är ett exempel hämtat från en artikel som handlar om bedrägeri:

”När kontot väl är kapat startar personen en chatt med dig, där han eller hon utger sig för att vara den verkliga ägaren. Snart styrs konversationen in på att vännen sitter och försöker betala sina räkningar, men inte hittar dosan till sin nätbank. Därför ombes du att hjälpa till genom att plocka fram din egen.” (4 nätbedrägerier som banken vägrar ersätta 2013).

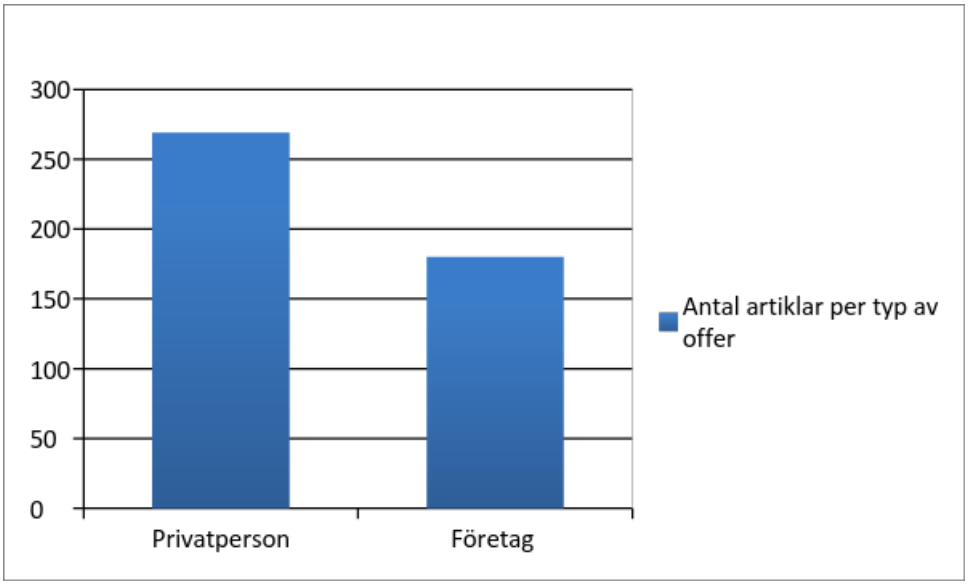
Enligt polisens definition kan phishing, skimning och trojaner alla vara metoder för att i slutändan begå ett bedrägeri. Phishing innebär exempelvis att förövaren på olika sätt försöker lura offret att avslöja uppgifter om sig själv medan skimning är ett samlingsbegrepp för när gärningsmannen manipulerar betalkortsautomater och bankomater för att komma åt information från kortremsan. En trojan är slutligen en skadlig kod som används för att ta sig in i offrets dator för att komma åt exempelvis koder och personlig information, ofta i syfte att begå ett bedrägeri.

Enligt Brottsförebyggande rådet, Brå, anmäldes 129 063 bedrägeribrott 2012, 148 362 anmäldes 2013 och 156 087 anmäldes 2014. Mellan 2013 och 2014 innebär detta en ökning med 5 procent vilket ska jämföras med datorbedrägerierna som under samma period har ökat med 25 procent. Brå menar att ökningen i utsatthet för bedrägerier till stor del beror på att internetanvändningen har ökat och att den tekniska utvecklingen bidrar till att det är möjligt att begå allt fler olika typer av bedrägerier. (Brå 2015 anmälda brott)

Trenden för artiklar då kategorierna datorbedrägeri, bedrägeri, phishing, skimning och trojaner slås ihop ser ut enligt följande för 2012, 2013 och 2014.



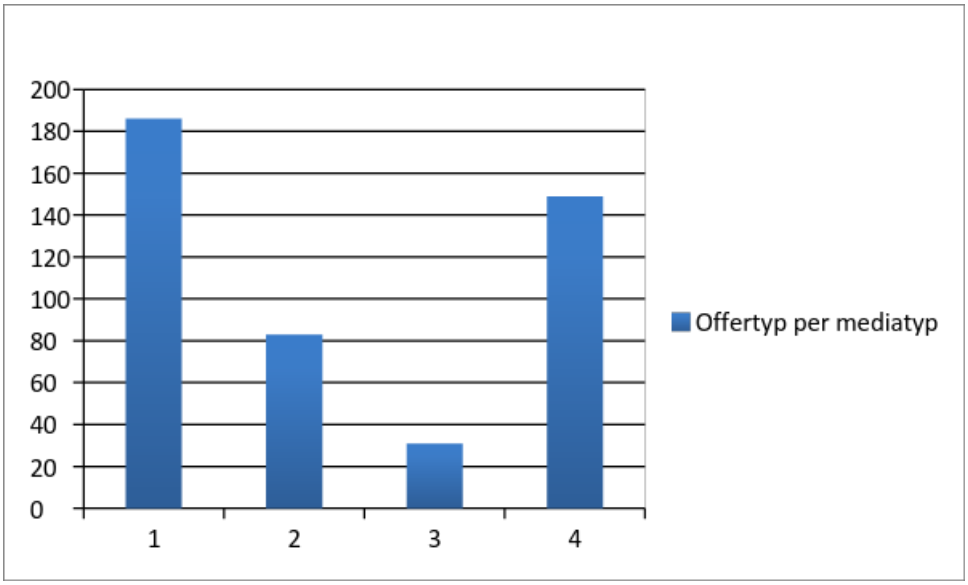
En annan aspekt som undersökts i artiklarna är om det är en privatperson eller ett företag (inklusive offentliga organisationer) som har blivit utsatt för brottet.



Artiklar som handlar om privatpersoner, 269 till antalet, som utsätts för IT-relaterade brott dominerar jämfört med artiklar där företag eller offentliga organisationer, 180 till antalet, utsatts för brott. Artiklar där alla offertyper finns med är ofta allmänna artiklar inom området. Följande citat är hämtat från en allmän artikel:

”Någon exakt statistik som räknar in alla brott med it-koppling finns inte att få tag på. Till exempel räknas häleri som sker genom sajter som Tradera eller Blocket i Brås statistik som just häleri, inte som en form av it-brottslighet.” (Dramatisk ökning av it-brott 2012)

En intressant skillnad mellan artiklar från Aftonbladet och IDG är att Aftonbladets artiklar nästan uteslutande handlar om brott där privatpersoner är offer medan IDG har många artiklar där också såväl företag som offentliga organisationer är offer.



Följande är ett citat från en typisk artikel från IDG:

”Det öppnar för att det rör sig om en hackare som planlöst söker efter säkerhetshål att utnyttja, oavsett var de upptäcks. I så fall skulle dataintrånget kunna vara helt opolitiskt. Att det riktas mot Alliansen just i valrörelsens slutskede skulle i så fall kunna vara en ren slump.” (Alliansens webbplats hackades 2014)

Nästa citat är hämtat från artikel ur Aftonbladet:

”16-åringen har nekat till brott men har erkänt att statusuppdateringen funnits på hans Facebooksida. Han ska tidigare ha sagt till Jönköpingsposten att han inte hade menat att kränka någon och att han själv har kompisar på Facebook som kommer från Somalia.” (Pojke dömd för rasistiskt Facebookinlägg 2013)

Reliabilitet, validitet och etiska överväganden

Reliabilitet eller tillförlitlighet handlar i huvudsak om resultatet av en undersökning blir detsamma om undersökning genomförs igen eller om resultatet kan påverkas av slumpmässiga eller tillfälliga betingelser (Bryman 2008, s. 49).

I den här uppsatsen har ett program använts för att hitta artiklar med relevans inom området IT-relaterade brott. Så länge programmet och nyckelorden som använts för sökningen inte förändras kommer en ny sökning vid ett annat tillfälle med stor sannolikhet ge samma resultat. Alla artiklar är hämtade från internet vilket i sig kan innebära en viss osäkerhet med tanke på att materialet kan försvinna eller förändras. Sammanfattningsvis borde reliabiliteten i

undersökningen vara hög då artiklarna inte har söks fram manuellt utan med ett automatiserat förfarande.

Validitet handlar om att bedöma om slutsatserna i en undersökning hänger ihop eller inte. Mätningsvaliditet eller begreppsvaliditet är vanligast när det gäller kvantitativa studier och går ut på att bedöma om redovisade mått verkligen står för de begrepp som de antas säga något om (Bryman 2008, s.50).

Mätningsvaliditeten hänger ihop med reliabiliteten och i den här uppsatsen har vi en fördel av det då vi bedömer att undersökningen har en tämligen hög reliabilitet. Däremot innebär den blandade användningen av begrepp när det gäller IT-relaterad brottslighet att ibland ett begrepp kan beskriva olika saker och ibland kan samma begrepp ingå i något annat begrepp. Det här påverkar validiteten i uppsatsen.

När det gäller de etiska principerna om informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet har vi inte behövt göra några särskilda hänsynstaganden i den här uppsatsen då den uteslutande bygger på datainsamling från redan publicerade artiklar (Bryman 2008, s. 131-32).

Sammanfattning

Under perioden 2012-2014 har artiklar som handlar om IT-relaterade brott legat mellan 150 – 250 artiklar per år från Aftonbladet respektive IDG med något fler från IDG.. När det gäller de olika brottstyperna, definierade av polisen, dominerar datorintrång, näthat och hackning och intrång. Minst vanliga är artiklar om gromning, barnpornografibrott, skimning och datorbedrägerier. Flera av de andra brottstyperna kan däremot resultera i ett bedrägeri enligt brottsbalkens 9 kapitel.

Den största skillnaden mellan artiklar från Aftonbladet och artiklar från IDG är att offren som beskrivs i Aftonbladet oftast är privatpersoner medan IDG också har en hel del artiklar där offren är företag och offentliga personer.

Lite kuriosa i sammanhanget är att en enskild händelse står för 45 av alla artiklar i undersökningen. Det är händelsen då Pirate Bay-grundaren Svartholm Warg begick ett dataintrång mot Skatteverket. Följande är ett exempel på citat från en sådan artikel:

”Två män i 30-årsåldern misstänks för intrång mot Logica, som lagrar uppgifter från Skatteverkets folkbokföring. Under våren har ett stort antal personnummer tillhörande personer med skyddad identitet läckt.” (Två misstänks för intrång mot Skatteverket 2012)

Diskussion och analys

I den här uppsatsen har vi valt att undersöka om det finns någon skillnad mellan hur olika typer av media, Aftonbladet.se och IDG.se, väljer att rapportera nyheter om IT-relaterade brott. Ett stort antal artiklar har samlats in från Aftonbladet.se och IDG.se för att sedan analyseras utifrån ett i förväg fastställt kodningsschema.

Brott och brottslighet handlar om en typ av skandaler där handlingen är exceptionell och där gärningsmannen/männen inte beter sig på ett acceptabelt sätt. Det här gäller traditionella brott likväl som de IT-relaterade brott vi har valt att fokusera på i den här uppsatsen. Vidare finns det en koppling mellan skandaler och de artiklar om skandaler som har möjlighet att få en stor läsekrets intresserad av innehållet. Det gäller dessutom att läsarna inte förkastar skandalen utan att intresset består och att skandaletiketten därmed bevaras (Wästerfors 2008, s. 75-76).

En analys av varför det är fler artiklar med IT-relaterade brottsskandaler i IDG.se jämfört med Aftobladet.se under perioden 2012-2014 handlar om att IDG.se är en samlingssida med nättidningar som uteslutande har fokus på en teknikorienterad publik. En publik som har lätt att uppfatta exempelvis ett dataintrång eller en hackingattack som en sådan exceptionell handling som också kan uppfylla kraven för att klassificeras som en skandal. När det gäller Aftobladet.se är det i stället en nätsida där de IT-relaterade brottsskandalerna får konkurrera med bland annat traditionella brott och rättegångar.

Det är snarare rimligt att tro att ett IT-relaterat brott kan uppfattas mer subtilt i samband med den interaktion som sker med den genomsnittlige läsaren av Aftonbladet. Det IT-relaterade brottet i det här fallet kan kanske uppfattas i förbifarten då läsaren är intresserad av något helt annat (Åkerström 2008, s. 81).

Att det förekommer fler artiklar där privatpersoner är offer än där företag eller offentliga organisationer är offer kan säkerligen förklaras av hur exceptionell händelsen uppfattas av publiken. Samtidigt måste också det förtroendebrott som gärningsmannen åstadkommer var tillräckligt stort. Att en grov kränkning på nätet av en ung utsatt person blir en tillräckligt exceptionell händelse med ett stort förtroendebrott såväl för läsaren av Aftonbladet.se som för läsaren av IDG.se är inte svårt att föreställa sig. Att ett intrång i ett centralt system hos ett större svenskt börsföretag är ett IT-relaterat brott som inte lika lätt kan uppnå och bibehålla en skandalstatus är på samma sätt inte heller svårt att föreställa sig. Analysen visar därmed att

skandalteorin även kan användas för att förklara skillnaden när det gäller vilka offer som förekommer i artiklarna om de IT-relaterade brotten (Wästerfors 2008, s. 74-75).

Att artiklarna med IT-relaterade brott i Aftobladet.se nästan uteslutande handlar om brott där privatpersoner är offer är inte heller konstigt med tanke på den blandade publik som utgör läsekretsen till Aftobladet.se. För Aftonbladets redaktion krävs förmodligen ett mycket exceptionellt IT-relaterat brott mot ett företag eller en offentlig organisation för att det ska bli en tillräcklig skandal för att vara värd att publicera.

Analysen av att så många som 45 artiklar handlar om dataintrånget mot Skatteverket blir att den händelsen och det förtroendebrott Pirate Bay-grundaren Svartholm Warg begick uppfyllde grundkraven för att klassificeras som en skandal. Dessutom måste tidningarna ha uppfattat att läsarna var villiga att bevara skandaletiketten med tanke på följetongen av nya artiklar om samma händelse (Wästerfors 2008, s. 75-76).

Även om skandalteorin inte ensam kan användas för att förklara varför media väljer att publicera artiklar om IT-relaterade brott finns sedan länge andra förklaringar som hjälper till att förstärka det publicistiska intresset. Sedan flera år tillbaka har nyhetsmedia hjälpt till att förstärka den allmänna oron för hot på nätet och andra IT-relaterade brott. Det här gäller inte bara traditionella pappersbaserade media utan även i allra högsta grad TV, radio och Internetbaserade nyhetsmedia som Aftonbladet.se och IDG.se (Yar 2013, s. 3-4).

Länge har IT-relaterade brottslighet varit helt förknippad med hackning, vilket är en aktivitet som till lika delar skapar fruktan som fascination hos allmänheten. Rent objektivt går det också att bekräfta att hackning innebär en väldigt skadlig IT-relaterad brottslighet. Trots detta finns det en hel del analytiker som hävdar att hotet från hackers är överdrivet och att det tenderar att också bli uppblåst i media. Själva fenomenet hackning och hackers är ur ett socialt perspektiv ett svar på den snabba tekniska utvecklingen. En utveckling där tekniken ofta representerar ett hot mot människans existens och där flera kända böcker och filmer hjälper till att förstärka den här bilden (Yar 2013, s. 24).

IDG.se är en hemsida med ett antal IT-relaterade tidningar som fokuserar på nyheter kring den tekniska utvecklingen inom området. I det perspektivet är det inte så konstigt att nyheter som rör dataintrång och hackning blir publicerade då de, som Yar, beskriver är en del av myten kring hackning och hackers.

Yar beskriver vidare att den sociala representationen av hackers och hackning inte bara är negativ utan att allmänheten även fascineras av fenomenet. Vid studier av publikreaktioner har bilden av den unga, smarta, hackern oftast kunnat kopplas till positiva reaktioner. Igen blir hackern något av en intelligent och beundrad hjälte när det gäller att bemöta hotet från den accelererande IT-utvecklingen. Yar menar också att hackning egentligen är en generell term för ett antal aktiviteter som rör intrång och manipulation av datorer. En term som representerar såväl hackning och intrång som dataintrång (Yar 2013, s. 26-27).

När Brottsförebyggande rådet publicerar den preliminära statistiken över anmälda brott 2014 framgår det att datorbedrägerier har ökat med 25 % från 2013 och att dataintrång har minskat med 28 %.

Urval av brottstyper som ökat 2014	Förändring jämfört med 2013		Urval av brottstyper som minskat 2014	Förändring jämfört med 2013	
	Antal	Procent		Antal	Procent
Skadegörelse, inkl. grov	+ 9 940	+ 7 %	Dataintrång	– 3 060	– 28 %
Datorbedrägeri	+ 8 490	+ 25 %	Bidragsbrott mot Försäkringskassan	– 1 770	– 35 %
Cykelstöld	+ 4 810	+ 7 %	Överlåtelse av narkotika	– 1 640	– 16 %
Ofredande	+ 2 760	+ 5 %	Utpressning	– 1 320	– 26 %
Olaga hot	+ 2 680	+ 6 %	Fickstöld	– 1 310	– 2 %

Brå: Anmälda brott 2014, preliminär statistik. Publicerad 2015-01-15.

Detta är en utveckling som inte är representativ för vårt urval av artiklar då vi tvärtom noterar ett minskat antal artiklar som rör datorbedrägerier, bedrägerier, m.fl. mellan 2013 och 2014. Vi är inte de enda att notera en avvikelse mellan faktiska brottsnivåer och rapporteringen i media. Sådant agenda-sättande beror oftast på pragmatiska hänsyn, det vill säga en hänsyn till vilket ämne som säljer bäst. (Yewkes 2014, s. 41) Man vädjar till läsarens begär och dramatiserar relativt ovanliga brott men tonar ned det som mer troligen ska hända. (ibid, s. 69)

Värt att notera är att Brå:s statistik handlar om den faktiska brottstypen datorbedrägeri medan vi använder såväl datorbedrägeri som IT-relaterade bedrägerier i vidare bemärkelse. Ökningen när det gäller bedrägerier förklara Brå beror till stor del på att internetanvändningen ökar och

att ny teknik innebär nya möjligheter att begå bedrägerier. En övergripande tendens är att brottsligheten går från stöldbrott till bedrägeribrott och att bedrägerier också utgör en ny typ av vardagsbrottslighet (Brå 2015 Anmälda brott 2014)

En bakomliggande förklaring till att antalet artiklar som handlar om bedrägerier sjunker kan ju vara att bedrägerierna blir mer och mer av vardagsbrottslighet, d.v.s. mindre fascinerande och skandalösa och därmed inte heller lika intressanta för Aftonbladet och IDG.

Vi nämnde hur oproportionerligt många gånger en viss Gottfrid Svartholm Warg och dennas turer i rättsväsendet förekommit bland de insamlade artiklarna. Det passar väl in i medias tendens att bevaka händelser som förutsägbara, det vill säga är lätta att planera för och avsätta resurser till. En rättegångs omfattning kan enkelt uppskattas och resurser avsättas. Vinklingen av hur ett visst nyhetsområde presenteras förändras sällan med tiden. Har rapporteringen börjat på ett visst sätt fortsätter den oftast åt samma håll. (Yewkes 2014, s. 46)

Vid sidan av hackning och datorintrång som varit ett huvudsakligt tema för artiklarna i IDG.se så har Aftonbladet.se publicerat fler artiklar där en privatperson har varit offret. En stor andel av artiklarna, 84 stycken, har handlat om brott som polisen sammanfattar under benämningen näthat. För att jämföra om vårt resultat är representativt använder vi senaste resultaten från en nyligen publicerad rapport från Brå som handlar om polisanmälda hot och kränkningar mot enskilda personer via internet.

Brå inleder med att bekräfta att hot och kränkningar via internet har fått allt större uppmärksamhet inte bara från media utan även från skola och politiker. När det gäller begreppet konstateras det att media, precis som polisen, använder termen ”näthat” medan skolan i stället ofta använder termen ”nätmobbing”. Vidare saknas det en samlad bild av de olika typer av hot och kränkningar mot enskilda personer via internet som anmäls till polisen och hur rättsväsendet hanterar brotten (Brå 2015, s. 5).

Underlaget för Brås studie är polisanmälda olaga hot, ofredanden, fridskränkningsbrott (grov fridskränkning och grov kvinnofridskränkning), olaga förföljelse samt ärekräkningsbrott (förtal och förolämpning). Då polisens ärendehanteringssystem inte tar hänsyn till om en händelse har skett via internet eller inte har Brå använt en sökordslista för att söka i de fritexter som skrivs in vid en brottsanmälan (Brå 2015, s. 7-8).

Brå kommer bland annat fram till att när målsäganden är ung så är ofta den utpekade gärningsmannen jämnårig. Pojkar har oftast utsatts för någon typ av hot om våld medan flickorna hängts ut med bilder på internet. För de ärenden som har granskats är personuppklaringen låg och den vanligaste anledningen till att ärendena ofta läggs ner är någon form av utrednings- eller bevissvårigheter (Brå 2015, s. 8-13).

Tyvärr har inte Brå valt att visa på någon statistisk utveckling, vilket beror på att det inte är möjligt att få fram information om hur stor andel av de anmälda brotten som begås via internet eller som på något annat sätt är IT-relaterade. Brå ansvarar för den officiella kriminalstatistiken och har i ett regleringsbrev för 2015 fått i uppdrag av regeringen att kartlägga utvecklingen av IT-relaterade inslag i anmälda brott (Brå 2015, s. 18).

Då Brå saknar statistik för IT-relaterad brottslighet kan vi inte bekräfta vårt resultat när det gäller antalet artiklar om näthat. Däremot är det helt klart att näthat är en vanligt använd term när det gäller hot och kränkningar mot enskilda personer via internet.

Avslutningsvis har vi i den här uppsatsen kunnat konstatera att Aftonbladet och IDG.se har publicerat mellan ca 150 – 200 artiklar vardera årligen under perioden 2012-2014. Den kvantitativa studien ger inte något stöd för ett särskilt samlingsbegrepp, men uppsatsförfattarna förordar trots detta att samlingsbegreppet IT-relaterade brott bör användas. Vidare handlar Aftonbladets artiklar nästan uteslutande om brott där privatpersoner är offer medan IDG även har flera artiklar där företag och offentliga organisationer är offer. En skillnad som borde kunna förklaras av den huvudsakliga publiken för respektive typ av media. Aftonbladet har en publik som utgörs av privatpersoner där den ”säljande” skandalen också mer naturligt är en händelse där en privatperson är offret medan IDG.se har en publik som i högre grad utgörs av företag och offentliga organisationer eller de som är intresserade av teknik i relation till företag. Avgörande för vilka IT-relaterade brott som rapporteras av respektive tidning blir följaktligen vad publiken uppfattar som en skandal (Wästerfors 2008, s. 74-75).

Förslag till framtida forskning

I den här uppsatsen har vi studerat en tidning på webben, och ett antal tidningar med teknisk inriktning under samma mediehus. En framtida utredning med större resurser än vår skulle kunna granska andra tidningar och media inom Sverige, eller använda samma uppställning internationellt. Något som vi inte alls gjort en ansats att hantera är de sociala media som idag

används och syns överallt. Till exempel skulle Twitter kunna bevakas automatiskt med ett program under en viss tidsrymd.

Referenslista

Artiklar

Levi Michael (2008). White-collar, organised and cyber crimes in the media: some contrasts and similarities Published online. *Springer Science + Business Media B.V. 26*.

Wall David S. (2008) Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law*.

Finnie T., Petee T., Jarvis J. (2010). The Future Challenges of Cybercrime: Volume 5.

Artiklar från Aftonbladet eller idg.se

Jenselius, Michael. 2012. *EU satsar inte tillräckligt på att bekämpa cyberbrott*. ComputerSweden. 27 november. http://computersweden.idg.se/2.2683/1.479154/eu-satsar-inte-tillrackligt-pa-att-bekampa-cyberbrott?queryText=cyberbrott (Hämtad 2015-04-12).

Kirkhoff, Emma. 2013. *Pojke dömd för rasistiskt Facebookinlägg* . Aftonbladet. 4:e juli. http://www.aftonbladet.se/nyheter/article17075005.ab (Hämtad 2015-04-12).

Larsson, Lius. 2013. *4 nätbedrägerier som banken vägrar ersätta*. PC för Alla. 8. http://pcforalla.idg.se/2.1054/1.508553/4-natbedragerier-som-banken-vagrar-ersatta?queryText=bedr%25C3%25A4geri%20internet (Hämtad 2015-04-12).

Larsson, Linus. 2014. *Alliansens webbplats hackades*. Internetworld. 2:a september. http://internetworld.idg.se/2.1006/1.581000/alliansens-webbplats-hackades?queryText=dataintr%C3%A5ng (Hämtad 2015-04-12).

Lindkvist, Ida. 2012. *Dramatisk ökning av it-brott*. ComputerSweden. 2:a februari. http://computersweden.idg.se/2.2683/1.430764/dramatisk-okning-av-it-brott?queryText=IT-brott (Hämtad 2015-04-12).

Ryberg, Jonas (2013). *Så hackades Logica*. ComputerSweden. 29:e april. http://computersweden.idg.se/2.2683/1.505012/sa-hackades-logica?queryText=bedr%25C3%25A4geri%20identitet (Hämtad 2015-04-12).

Videla, Emanuel. 2012. *Två misstänks för intrång mot Skatteverket*. ComputerSweden. 14:e juni. *http://computersweden.idg.se/2.2683/1.454229/tva-misstanks-for-intrang-mot-skatteverket?queryText=dataintr%C3%A5ng* (Hämtad 2015-04-12).

Böcker

Bryman Alan (2008). *Samhällsvetenskapliga metoder.* Lund: Liber.

Jewkes Yvonne (2011). *Media & Crime*. Los Angeles: SAGE Publications.

Pollack Ester (2001). *En studie i medier och brott*. Stockholm: Stockholms Universitet.

Yar Majid (2013). *Cybercrime and society.* London: SAGE Publications.

Wästerfors, D. (2008). Skandalen och publiken. I Åkerström, M. (red.) *Medier, brott och den aktiva publiken.* Malmö: Bokbox förlag.

Åkerström, M. (2008). Media som diskursiv bakgrundsmusik. I Åkerström, M. (red.) *Medier, brott och den aktiva publiken.* Malmö: Bokbox förlag.

Övriga källor

Arrland et al (2015) Informations- och cybersäkerhetsutredningen (2015). Informations- och cybersäkerhet i Sverige - Strategi och åtgärder för säker information i staten (SOU 2015:23). Stockholm: Justitiedepartementet. http://www.sou.gov.se/wp-content/uploads/2015/03/SOU-2015_23_webb.pdf (Hämtad 2015-05-28)

Brå (2000). IT-relaterad brottslighet (Rapport 2000:2). Stockholm: Brå

Brå (2015). Polisanmälda hot och kränkningar mot enskilda personer på nätet (Rapport 2015:6). Stockholm. Brå

Brå (2015) webbsida, Anmälda brott. https://www.bra.se/bra/brott-och-statistik/bedragerier-och-ekobrott.html (Hämtad 2015-04-25)

Brå (2015) webbsid, Anmälda brott 2014. https://www.bra.se/bra/nytt-fran-bra/arkiv/nyheter/2015-01-15-anmalda-brott-2014---preliminar-statistik.html (Hämtad 2015-09-19)

Informations- och cybersäkerhetsutredningen (2015). Informations- och cybersäkerhet i Sverige - Strategi och åtgärder för säker information i staten (SOU 2015:23). Stockholm: Justitiedepartementet.

Bilagor

Rådata som använts i uppsatsen, med artiklar från Aftonbladet.se och IDG.se, kan laddas ner som separata bilagor,

i PDF-format:

https://aurorasystems.eu/aurora/share/medias_rapportering_av_it_relaterade_brott/keywords_aftonbladet_idg_2012-01-01_2015-01-01.pdf

i Excel-format:

https://aurorasystems.eu/aurora/share/medias_rapportering_av_it_relaterade_brott/keywords_aftonbladet_idg_2012-01-01_2015-01-01.xlsx

i SPSS-format:

https://aurorasystems.eu/aurora/share/medias_rapportering_av_it_relaterade_brott/keywords_aftonbladet_idg_2012-01-01_2015-01-01.sav

Lista över bortgallrade artiklar, irrelevanta eller dubbletter:

https://aurorasystems.eu/aurora/share/medias_rapportering_av_it_relaterade_brott/bortgallrade-artiklar-och-dubletter.xlsx